JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 12, pp. 171-178, December 2022
https://doi.org/10.9708/jksci.2022.27.12.171

# Classification and Risk Analysis of Stablecoins

Junsang Kim*

*Assistant Professor, Dept. of Cyber Science, Korea Naval Academy, Changwon, Korea

## [Abstract]

In this paper, we propose a classification method according to the type and characteristics of stablecoins for risk analysis, and analyze the risk factors of each stablecoin based on this classification.

First, this paper explains the technologies and ecosystem of blockchain and decentralized finance(DeFi) to understand stablecoins. In addition, the operation principle of the major stablecoins currently released and used is explained for each proposed classification type. Based on this, the risk type and risk factors of each stablecoin are derived.

The risk types proposed in this paper are classified as defegging, liquidation, and exploit, and the risk factors are classified as depegging due to reliability of operator, depegging due to reliability of algorithm, depegging due to failure of algorithm, liquidation due to high volatilty and oracle attack. Based on the proposed classification, we analyze the risk factors of major stablecoins currently circulating in the crypto market.

▸ **Key words**: Blockchain, Cryptocurrency, Stablecoin, Decentralized Finance, DeFi

## [요 약]

본 논문에서는 스테이블코인의 위험 분석을 위해 스테이블코인의 유형과 특징에 따른 분류방법을 제안하고 이를 토대로 각 스테이블코인들의 위험요인들을 분석한다.

먼저, 본 논문에서는 스테이블코인의 이해를 위해 블록체인 및 탈중앙화 금융(Decentralized Finance, DeFi)의 기술들과 생태계에 대하여 설명한다. 그리고 현재 출시되어 사용되고 있는 주요 스테이블코인의 동작원리에 대하여 제안한 분류 유형별로 설명한다. 이를 토대로 각 스테이블코인의 위험형태와 위험요인을 도출한다.

본 논문에서 제안하는 위험형태의 분류는 디페깅, 청산, 취약점 공격이며 위험요인의 분류는 운영자의 신뢰성 문제로 인한 디페깅, 알고리즘의 신뢰성 문제로 인한 디페깅, 알고리즘 오류로 인한 디페깅, 급격한 가격변동으로 인한 청산, 그리고 오라클 공격이다. 제안하는 분류를 기준으로 현재 암호화폐 시장에서 유통되는 주요 스테이블코인들의 위험요인을 분석한다.

▸ **주제어**: 블록체인, 암호화폐, 스테이블코인, 탈중앙화 금융, 디파이

• First Author: Junsang Kim, Corresponding Author: Junsang Kim
*Junsang Kim (junsang.kim@navy.ac.kr), Dept. of Cyber Science, Korea Naval Academy
• Received: 2022. 11. 30, Revised: 2022. 12. 23, Accepted: 2022. 12. 23.


http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

## I. Introduction

2022년 5월 경 테라USD(UST)의 가격이 1달러 이하로 떨어지면서 이를 뒷받침해주던 코인인 시총 5위 암호화폐인 루나(LUNA)가 대폭락한 사건이 발생하였다[1]. 이 사건으로 시총 52조원이 증발하면서 국내외 수많은 피해자들이 발생되었고 세계적인 암호화폐 대부업체인 셀시우스 네트워크(Celsious Network)와 한때 자산이 100억달러에 이르렀던 대형 암호화폐 헤지펀드인 쓰리에로우캐피탈(3AC)이 파산하였다. 국내 암호화폐 펀드 운용업체인 헤이비트(Heybit) 또한 267억원 규모의 암호화폐 투자펀드가 강제로 청산당하는 등 LUNA 폭락 사태는 국내외 엄청난 파장을 일으켰고 그 여파가 지금까지 시장에 지속되고 있다.

LUNA 폭락 사태 이전에도 스테이블코인의 안정성에 대하여 많은 이슈가 있었다. 대부분의 스테이블코인은 이를 뒷받침하는 담보를 기반으로 가치를 유지하는데, 이 담보의 신뢰성이 훼손되는 경우가 대표적이다. 달러 자산을 담보로 하는 최초의 스테이블코인인 테더(USDT)는 계속해서 담보의 신뢰성 논란이 있었고, 시장에서는 이를 테더 리스크라 불리며 이 문제가 부각될 때마다 암호화폐 시장에 충격을 가져다주었다.

테라 블록체인 네트워크에서 발행한 UST는 실물 담보가 없이 자매 코인인 LUNA의 발행량을 조절하는 알고리즘으로 가격을 유지하는 스테이블코인으로 실물 담보를 기반으로 하는 다른 스테이블코인에 비해 근본적으로 안정성이 취약했다. 하지만 이러한 문제가 시장에 제대로 인식되지 못하면서 결국 전체 암호화폐 시장에 큰 충격을 주고 많은 피해자를 양산하게 되었다. 이렇듯 스테이블코인의 안정성이 손상되면 많은 피해자들이 발생하고 블록체인 생태계가 크게 손상되는 문제가 발생하기 때문에 위험요인을 발견하고 보완하여 보다 안정적인 스테이블코인 생태계로 발전해야 될 필요가 있다. 이를 위해 본 논문에서는 시중에 출시되어 유통되고 있는 주요 스테이블코인들을 소개하고 특징 및 유형별로 분류한 후 이를 토대로 각 스테이블 코인의 위험 요인에 대해서 분석하고 설명한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 스테이블코인의 기반 기술인 블록체인, 스마트 계약, 탈중앙화금융 등에 대해서 설명한다. 그리고 3장에서는 주요 스테이블코인에 대하여 설명하고 이를 특징과 유형별로 분류한다. 4장에서는 이를 토대로 각 스테이블코인의 위험요일을 분석한 후 5장에서는 결론을 맺는다.

## II. Background Technology

### 1. Bitcoin & Blockchain

블록체인 기술은 2008년 나카모토 사토시(Nakamoto Satoshi)라는 신원미상의 인물이 비트코인(BTC)이라는 암호화폐를 제안하면서 시작되었다[2].

블록체인은 수많은 노드(Node)가 인터넷 기반의 P2P 네트워크로 연결되어 거래를 기록하고 처리하는 '분장 원장 시스템'이다. 사토시는 BTC의 생성과 거래의 위조를 방지하기 위해 블록체인 기술을 고안하였으며 현재는 암호화폐 분야뿐만 아니라 데이터 신뢰 및 위변조 방지가 필요한 많은 분야에 널리 사용되고 있다. 일반적으로 금융거래는 은행과 증권사와 같은 신뢰성 있는 중개자가 운영 및 보증하는 역할을 하지만 블록체인은 중개자 없이 다양한 참여자들이 원장을 공동으로 기록하고 관리하여 원장의 신뢰성을 보증한다. 어떠한 거래기록이 발생하면 모든 참여자의 합의에 의해 공통의 원장에 기록되기 때문에 조작이 불가능하다. 이 원장은 Fig 1과 같이 블록으로 이루어진 연결리스트로 이전 블록의 해시값이 다음 블록에 포함되기 때문에 특정 블록의 변조가 불가능하다[3].

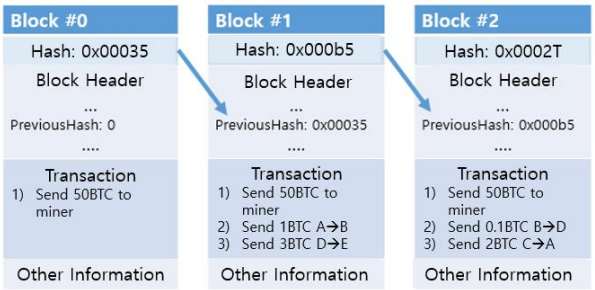


Fig. 1. Blockchain Architecture[3]

### 2. Ethereum & Smart Contract

스마트 계약은 계약을 프로그래밍하여 블록체인에 탑재할 수 있는 기술로 중개자 없이 특정 요건에 도달했을 경우 자동으로 프로그래밍 된 계약이 실행이 된다. 암호자산을 맡겼을 때 자동으로 이자가 지급되게 하거나, 특정 암호화폐를 보내면 다른 암호화폐를 일정 비율로 교환하는 등 다양한 금융거래를 스마트 계약으로 구현할 수 있다. 스마트 계약은 은행이나 증권사와 같은 신뢰성 있는 중개자가 없지만 많은 노드들에 의해 영구히 기록되고 조작이 거의 불가능하기 때문에 계약 실행의 보증이 가능하다.

스마트 계약은 2015년 비탈릭 부테린(Vitalik Buterin)이 개발한 암호화폐인 이더리움(ETH)을 기반으로 최초로

개발되었다[4]. BTC가 화폐거래 트랜잭션만을 블록체인에 기록할 수 있었다면 ETH는 다양한 형태의 계약을 솔리디티(Solidity)라는 프로그래밍 언어의 코드로 만들어 블록체인에 기록할 수 있다. ETH 이후 개발된 블록체인 네트워크는 대부분 스마트 계약을 지원하고 있다. 스테이블코인도 대부분 자체적인 블록체인 네트워크를 가지고 있는 것이 아니라 ETH와 같은 블록체인의 스마트 계약을 이용하여 토큰(Token)으로 발행되고 소각되는 형태로 구현되어 있다. 시중에 유통되는 대부분의 스테이블코인은 ETH 기반의 토큰이지만 솔라나(SOL), 바이낸스 스마트체인(BSC), 폴리곤(MATIC) 등의 블록체인 네트워크를 통해서도 스테이블코인이 발행되고 있다.

## 3. Decentralized Finance (DeFi)

BTC를 개발한 나카모토 사토시는 기존 은행 시스템에 대한 불신을 가지고 있었기 때문에 은행과 같은 중앙집중적인 기관이 없이도 견고한 금융시스템을 BTC를 통해 구현하고자 했다. 사토시가 구현한 BTC는 암호화폐의 생성과 거래, 그리고 검증의 기능을 제공한다. 예금, 대출, 보험, 파생상품 등 복잡한 금융 계약이 필요한 서비스들은 BTC 상에서는 구현이 불가능했다. 하지만 스마트 계약을 블록체인 상에서 구현할 수 있는 암호화폐인 ETH가 개발되면서 중개자 없는 금융, 즉 탈중앙화 금융(DeFi)의 구현이 가능해졌다[5]. DeFi의 생태계를 이루는 대표적인 구성요소들은 다음과 같다.

### 3.1 Crypto Wallet

DeFi를 이용하기 위해서는 우선 개인 암호화폐 지갑이 있어야 된다. 암호화폐 지갑은 블록체인 네트워크마다 다르며 해당 네트워크를 개발 및 운영하는 재단(Foundation)에서 소프트웨어 형태로 배포하는 경우가 많다. 이더리움 네트워크의 경우 메타마스크(Metamask)가 가장 많이 쓰인다. 개인 지갑을 설치하면 개인의 고유 주소가 생성되며 이를 이용하여 계좌번호처럼 입출금이 가능하다. 지갑의 주소가 생성될 때 개인 키(Private key)도 함께 생성되는데 암호화폐 출금이나 스마트 계약 실행 시 개인 키로 서명하여 거래를 승인한다. 개인 키는 브라우저에 저장이 되며 좀 더 보안성을 강화하기 위해 하드웨어에 개인키를 저장할 수 있는 하드웨어 지갑들도 시중에 출시되어 있다.

### 3.2 Decentralized Exchange(DEX) Protocol

탈중앙화 거래소(DEX)는 중개기관 없이 내 지갑에서 바로 암호화폐의 거래가 가능한 프로토콜이다. 업비트나 바이낸스 등 중앙화된 거래소는 내 지갑에서 거래소 지갑으로 암호화폐를 송금하거나 법정화폐로 구매해야 암호화폐를 거래할 수 있다. 그러므로 거래소가 폐쇄되거나 서비스가 중단되었을 때는 거래가 불가능하다. 또한 블록체인 네트워크상에서 암호화폐의 소유자는 거래소가 되므로 거래소 폐쇄나 도산 시 암호화폐를 돌려받을 수 없는 경우도 발생한다. 탈중앙화 거래소는 내 지갑에서 바로 블록체인 네트워크를 통해 거래가 되므로 이러한 문제에서 자유롭다.

탈중앙화 거래소는 자동화된 마켓 메이킹(Automated Market Making, AMM) 기술을 이용하여 구현된다. AMM은 수익을 얻기 바라는 유동성 공급자(Liquidity provider)들이 모여 유동성 풀을 만들고 미리 구현되어 있는 스마트 계약에 의해 자동으로 결정된 가격으로 거래를 가능하게 한다[6]. 대표적인 탈중앙화 거래소는 유니스왑(Uniswap)과 스시스왑(Sushiswap)이 있다[5].

### 3.3 Lending Protocol

랜딩 프로토콜은 중개기관 없이 내 지갑에서 바로 암호화폐를 맡기거나 빌릴 수 있는 예금/대출 프로토콜이다. 대표적인 랜딩 프로토콜은 MakerDAO, Compound, Aave등이 있으며 이 세 개의 프로토콜이 항상 총자산규모 상위 5위에 들 정도로 큰 규모의 자산을 보유하고 있다[5]. 암호화폐를 보유하고 있는 사용자는 랜딩 프로토콜에 자산을 맡겨 이자수익을 얻을 수 있으며 암호화폐를 담보로 일정기간 법정화폐가 필요한 사용자는 이를 담보로 스테이블코인을 빌려서 사용할 수 있다. 이러한 일련의 과정은 중개자 없이 스마트 계약으로 처리된다.

### 3.4 Oracle

블록체인의 오라클이란 블록체인 외부의 소스에서 수집한 데이터를 블록체인 안으로 가져오는 것을 의미한다. 대표적인 오라클 사용 사례는 가격 피드이다. 암호화폐 담보 스테이블코인이나 랜딩 프로토콜은 정해진 담보비율 아래의 대출건의 담보를 청산하게 되는데 이때 담보의 가격과 대출한 자산의 가격에 대한 데이터가 필요하다. 랜딩 프로토콜은 미리 작성된 스마트 계약을 블록체인 네트워크 위에 올려놓고 실행하는데 담보나 자산의 가격은 실시간으로 변동하므로 스마트 계약 작성 시 미리 입력할 수 없다. 그러므로 대표적인 거래소 등 외부의 데이터 소스로부터 지속적으로 신뢰성 있는 데이터를 입력받아야 하는데, 블록체인 생태계에서는 오라클을 이용하여 이 문제를 해결한다. 대표적인 오라클은 체인링크(LINK)[7]와 밴드프로토콜(BAND)[8]이 있다.

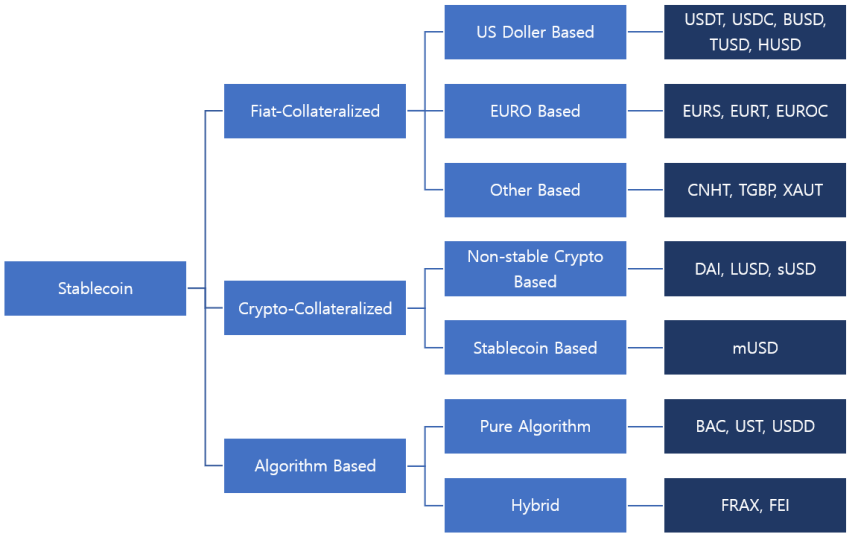


Fig. 2. Classification of Stablecoins

## III. Survey and Classification of Stablecoins

일반적인 암호화폐는 기본적으로 법정화폐보다 가격변동성이 높기 때문에 자산 보유자 입장에서는 항상 변동성에 노출되어 있다. 이러한 가격 변동성은 암호화폐 보유자의 위험도 관리와 실생활에서 암호화폐 사용에 큰 걸림돌이 되어왔다. 그래서 암호화폐 시장에서는 일정한 가치를 유지할 수 있는 스테이블코인의 필요성이 대두되었다[9-10]. 특히 암호화폐 지갑은 암호화폐만 입출금이 가능하므로 법정화폐의 보관이 불가능하다. 최초의 스테이블코인인 USDT는 미국 달러의 가격을 추종하는 코인으로 이로써 법정화폐의 가치에 준하는 스테이블코인을 암호화폐 지갑에 보관할 수 있게 되었다. 이는 블록체인 세계, 암호 화폐와 현실 세계, 법정 화폐 사이의 중개자 역할을 하여 블록체인에 기반한 금융 시스템인 DeFi의 발전을 가능하게 하였다.

현재 대부분의 스테이블코인은 미국 달러 기반으로 1달러의 가치를 가지고 있는데 가치의 유지를 위해 담보를 두고 발행하는 등 다양한 방법을 사용한다. 스테이블코인은 담보와 특성에 따라 크게 3가지로 분류할 수 있다[5]. 본 장에서는 스테이블코인의 특성과 유형에 따라 좀 더 세부적으로 분류한다. 분류한 결과는 Fig 2와 같으며 본 장에서는 그 결과에 대하여 설명한다.

### 1. Fiat-Collateralized Stablecoins

법정화폐 담보 스테이블코인은 미국 달러나, 유로 등의 실물화폐를 담보로 발행되는 스테이블코인으로 해당 실물화폐를 입금하면 스테이블코인을 토큰 형태로 발행(mint)하여 입금자의 개인지갑에 송금해주고 입금자가 이를 반환하면 코인을 소각하고 법정 화폐를 돌려주는 방식으로 운영된다. 이러한 스테이블코인은 홍콩의 Tether사에서 운영하는 테더(USDT), 테더EURT(EURT)과 미국의 서클(Circe)사가 운영하는 USD Coin(USDC), EURO Coin(EUROC)이 대표적이다. 그 외 미국 달러 기반의 스테이블코인으로는 바이낸스 거래소에서 발행하는 바이낸스USD(BUSD), 후오비 거래소에서 발행하는 후오비USD(HUSD), TrueUSD사에서 발행하는 TUSD 등이 있다. 그 외 영국 파운드화 기반의 TrueGBP(TGBP), 중국 위안화 기반의 테더CNHT(CNHT), 금 기반의 테더골드(XAUT)도 있다.

### 2. Crypto-Collateralized Stablecoins

암호화폐 담보 스테이블코인은 일반적으로 ETH와 같은 암호화폐를 담보로 하여 발행한다. 암호화폐는 가격 변동성이 크므로 담보의 가치보다 적은 스테이블코인을 발행할 수 있다. 그리고 담보로 제공한 암호화폐의 가치가 떨어져 적정한 담보비율을 유지하지 못하는 경우 자동으로 담보를 청산하여 손실을 회피한다. 그러므로 암호화폐 담보 스테이블코인은 태생적으로 담보의 가치보다 낮은 금액의 스테이블코인을 얻게 되는 없는 비효율성이 존재한다. DAI, LUSD는 ETH를 담보로 발행되며 sUSD는 자체 거버넌스 토큰인 신세틱스 네트워크 토큰(SNX)을 담보로 발행한다.

앞서 언급한 스테이블코인은 변동성 있는 암호화폐를 담보로 맡기는 형태였으면 여러 스테이블코인을 조합하여 또 다른 스테이블코인을 발행하는 형태도 존재한다. mStable사에서 발행하는 mUSD의 경우 법정화폐 담보

스테이블코인인 USDT, USDC와 암호화폐 담보 스테이블코인인 DAI, sUSD를 일정 비율로 혼합하여 mUSD를 발행한다. 다른 암호화폐 담보 스테이블코인과 달리 일반적인 상황에서는 담보의 가치와 발행된 mUSD의 가치는 동일하다. mUSD를 구성하는 담보들은 각각 5~50% 사이의 비율을 가지며 실시간을 변화된다. mUSD는 4개의 스테이블코인으로 담보되어 있어 각각의 위험요인을 분산할 수 있으며 담보를 탈중앙화거래소에 유동성으로 제공하여 거래수수료 수익을 창출할 수 있다는 장점이 있다.

### 3. Algorithmic Stablecoins

알고리즘 스테이블코인은 가격이 정해진 가격을 이탈할 때 알고리즘을 통해 정해진 가격으로 회복하는 구조를 가지고 있다. 알고리즘 스테이블코인은 크게 두 가지 유형으로 나눌 수 있는데 전혀 담보가 없는 BAC, UST, USDD와 담보를 알고리즘 형태로 사용하는 FRAX, FEI 등이 있다.

무담보형 스테이블 코인(Non-Collateralized Stable Coin)은 법정화폐나 다른 암호화폐에 의해서 담보되진 않지만 코인의 유통량을 화폐의 수요-공급의 법칙을 이용하여 조절하여 가격을 정해진 가격에 맞추도록 알고리즘이 구성되어 있다. 즉, 스테이블코인의 가격이 정해진 가격보다 상승했을 때 추가 발행하여 시중의 유통량을 늘리고 가격이 정해진 가격보다 하락하면 매수하여 소각하는 방식으로 가치를 조정한다. UST의 경우 자매 코인인 LUNA를 이를 조정하기 위한 자산으로 사용하는데 UST가 1달러보다 가격이 떨어지더라도 1달러치의 LUNA로 발행할 수 있다. 시장에 UST의 수요가 많아져서 가격이 1달러보다 높아지면 1달러치의 LUNA를 소각하여 UST 1개를 발행한다. 결국 사용자들은 UST의 가격이 떨어지면 LUNA를 싸게 교환하여 차익을 챙길 수 있고 UST의 유통량은 줄어든다. 반대로 UST의 가격이 오르면 사용자들은 보유한 LUNA를 소각하고 UST로 바꾸어 1달러를 초과한 금액의 차익을 챙기고 UST의 유통량은 늘어난다. 시장에서 UST의 수요가 많을수록 LUNA의 수요가 많아지고 LUNA가격은 점점 상승하게 된다. USDD는 TRON 블록체인 기반의 스테이블코인으로 기본적인 원리는 LUNA와 유사하지만 트론 블록체인의 기축통화인 트론(TRX)를 이용하여 USDD의 발행량을 조절한다.

최초의 알고리즘 스테이블 코인인 Basis Cash(BAC)도 UST와 유사한 구조를 가지고 있다. BAC의 가격이 1달러 밑으로 떨어졌을 때 1:1로 Basis Bond(BAB)로 교환할 수 있다. BAB는 추후 BAC의 가격이 1달러 이상으로 돌아왔을 때 다시 BAC로 교환이 가능하므로 BAC의 가격이 떨어진 만큼의 수익을 얻을 수 있다. BAC가 BAB로 전환되면 시중의 BAC 유통량이 줄어들어 가격상승을 도모할 수 있다. 가격 상승기가 길어져서 발행한 BAB가 모두 교환된 경우 BAC의 거버넌스 토큰인 Basis Share(BAS)의 보유자에게 BAC를 분배하여 시장의 BAC 유통량을 늘리고 가격하락을 도모하는 방식으로 가격을 조정한다,

하이브리드 방식의 알고리즘 기반 스테이블코인은 가격을 알고리즘으로 조정하지만 이를 뒷받침하는 담보도 있는 경우이다. FRAX의 경우 법정화폐 기반 스테이블코인인 USDC를 담보로 가격을 조정한다. FRAX의 가격이 1$ 이하인 경우에는 담보비율이 높아지며, FRAX의 가격이 1$ 이상이 되는 경우 담보비율이 낮아진다. FRAX의 담보비율은 현재 93% 수준을 유지하고 있고 최저점은 82% 선이다. 발생한 스테이블코인은 USDC로 그 가치를 100% 커버하지 못하지만 알고리즘에 의해서 1$ 가격이 유지되고 있다. FRAX는 담보비율이 90%인 경우 USDC 0.9$, FRAX Share(FXS) 0.1달러를 지불하고 교환할 수 있다, 시장에서 FRAX의 수요가 늘어나면 FRX의 수요가 늘어나게 되고 가격도 점점 상승하게 된다. 이때 FRAX의 발행에 필요한 FXS의 비율도 점점 높아지게 되어 USDC의 의존도가 낮아지게 된다. FRAX의 신뢰도가 높아져서 신뢰도가 상승하면 담보비율을 줄이고, 낮아지면 도 담보비율을 높여서 담보를 이용하여 1$의 가격을 유지하는 것이다. FRAX의 수요가 줄면 FXS의 가격은 하락하지만 FRAX의 가격 자체는 1$를 유지하도록 설계되어 있다.

FEI의 경우 ETH를 지불하고 발행할 수 있으나 ETH가 담보로 사용되는 것이 아니라 가격 유지를 자산으로 운용한다. 지불된 ETH는 유니스왑의 ETH/FEI 페어풀로 귀속이 된다. 만약 FEI의 가격이 1$이하로 상당기간 유지되는 경우 유니스왑풀에서 ETH를 인출한 후 FEI를 매입하여 유니스왑풀의 FEI 가격을 다시 1$ 가격으로 회복시키는 과정을 수행한다. ETH를 담보로 사용하는 것이 아니기 때문에 청산의 위험이 없고, ETH의 가치만큼 FEI를 발행할 수 있다는 장점이 있다.

## IV. Risk Analysis of Stablecoins

사용자 입장에서 스테이블코인의 발행이나 보유 시 자산의 손실이 발생하는 형태는 크게 3가지로 디페깅(Depegging), 청산(Liquidation), 취약점 공격(Exploit)으로 분류된다 본 장에서는 각각의 위험형태들을 정의하고 각 스테이블코인의 위험요인을 5가지로 나누어 분석한다.

## 1. Risk types of stablecoins

### 1.1 Depegging

디페깅은 스테이블코인의 정해진 가치를 이탈하는 경우를 말하는 것으로 일반적으로 1% 정도의 가격 변동은 디페깅으로 판단하지 않는다. 디페깅은 스테이블코인의 대표적인 위험요소로 다양한 원인으로 인해 단기간 디페깅이 발생하는 경우가 종종 발생하지만 만약 단시간에 회복되지 않으면 시장의 신뢰성을 잃어버려 가격 폭락 후 시장에서 퇴출되는 상황이 발생한다. 현재까지 대부분의 디페깅 이슈는 알고리즘 기반 스테이블코인에서 발생했다.

### 1.2 Liqudation

주로 암호화폐 담보 스테이블코인에서 발생하는 이슈로 대부분 담보로 맡긴 암호화폐의 가격이 낮아지면서 담보 비율을 맞추기 못해 담보가 청산되어 손실이 발생한다. 담보의 가격이 항상 빌린 자산에 비해 가치가 높기 때문에 담보가 청산되면 10~30% 정도의 손실이 발생한다. 담보 비율에 여유를 충분히 두고 스테이블코인을 발행하면 이러한 문제를 예방할 수 있지만 그렇지 못하다면 급격한 가격 변동 시 담보가 청산될 수 있다.

### 1.3 Exploit

취약점 공격은 암호화폐 플랫폼이나 스마트 계약의 버그를 이용하여 암호화폐를 탈취하거나 부당하게 취득하는 것을 의미한다. 탈중앙화금융 생태계에서 대표적인 취약점 공격은 오라클의 데이터 소스를 공격하여 조작하는 것과 스마트 계약 버그를 이용하여 허가받지 않은 자가 암호화폐를 탈취하는 것이다.

오라클 공격의 대표적인 사례는 오라클의 데이터 소스가 되는 특정 거래소에 비정상적인 거래를 시도해 특정 자산의 가격을 의도적으로 상승시키거나 하락시키는 것이다. 암호화폐 담보 스테이블코인 공급자가 이 특정 거래소와 연동되는 오라클의 가격 피드를 사용한다면 공격자는 비정상적으로 가격이 상승된 자산을 담보로 맡겨 고액의 스테이블코인을 인출할 수 있다. 이후 가격 피드가 정상으로 돌아와 공급자가 해당 담보를 청산하여도 공급자의 담보는 큰 손실을 입게 되어 발행한 스테이블코인의 신뢰도 하락으로 이어져 뱅크런 및 디페깅이 발생될 수 있다. 오라클 공격을 방어하기 위해 오라클은 데이터 소스를 다변화하고 이상치를 보이는 데이터 소스를 일시적으로 제외하는 등 다양한 방어수단을 도입하여 현재 오라클 공격이 성공하여 발생한 손실은 많이 줄어든 편이다.

DeFi에서 사용하는 스마트 계약은 프로그래밍 언어로 개발하기 때문에 버그가 발생할 수 있다. 만약 버그를 발견하지 못하고 블록체인 상에서 동작하게 될 때 이로 인한 암호화폐 탈취가 발생하는 경우가 발생한다. 예를 들어, 스테이블코인의 발행에 관련된 스마트 계약에 취약점이 있으면 해커가 이를 이용하여 스테이블코인을 무한히 발행하거나 일부를 탈취할 수 있다. 최근에는 탈중앙화금융 시장이 발달하면서 제품출시 전 스마트 계약 전문 감사업체들에게 감사를 받는 경우가 대부분으로 이로 인한 피해 금액도 점점 줄고 있다. 또한 고액의 버그바운티(Bug Bounty)제도를 운영하여 해커들이 불법적인 해킹으로 자금을 탈취하기보다 취약점을 신고하고 합법적으로 상금을 받아가도록 유도하고 있다.

## 2. Risk analysis by risk factor

### 2.1 Depegging due to reliability of operator

법정화폐 담보 스테이블코인은 기본적으로 중앙화된 시스템으로 운영되기 때문에 운영이나 권한을 탈중앙화하여 운영기관의 위험요인을 줄이는 블록체인의 취지와 맞지 않다. 이는 중앙화된 스테이블코인 운영사의 신뢰도나 담보물에 문제가 있을 경우 그 가치가 흔들릴 수밖에 없기 때문이다. 테더사에서 발행한 USDT의 경우 담보물의 운영 및 보유현황이 투명하지 않다는 지적을 자주 받아왔고 뉴욕 검찰, 미국 선물상품거래위원회 등의 기관의 조사로 인해 약간의 디페깅이 일어난 적도 있다. HUSD의 경우 모기업인 후오비 거래소가 흔들리면서 디페깅이 일어났고 현재까지 큰 폭의 디페깅이 유지중이다. 하지만 HUSD를 제외하고 주요 법정화폐 담보 스테이블코인 중에서 디페깅이 큰 폭으로, 또는 장기적으로 일어난 적이 없지만 향후 언제든지 해당 문제는 발생할 수 있다. 하지만 세계 여러 국가에서 추진 중인 CBDC(Central Bank Digital Currency)가 본격적으로 발행되면 기존의 중앙화된 스테이블코인을 대체하고 신뢰도는 법정화폐 수준으로 향상될 것으로 예상된다[11-12].

### 2.2 Depegging due to reliability of algorithm

담보가 없는 알고리즘 스테이블코인은 사용자들이 해당 코인의 가격 유지 알고리즘에 대한 신뢰를 잃었을 때 디페깅이 발생하여 가치를 상실할 수 있다. BAC의 경우 수요를 창출하는데 실패하였고 사용자의 신뢰를 얻지 못하여 사용자들이 BAB를 자율적으로 매수하여 가격을 조정하는데 실패하였다. UST의 경우 연간 20%의 이자를 지급하는 앵커프로토콜이라는 서비스로 인해 수요가 계속 상승하고 있었고 UST와 연동되는 LUNA는 테라 블록체인 네트워크

의 기축 암호화폐로서 사용 용도와 가치가 있었다. 하지만 UST는 22년 5월 디페깅이 발생하였는데, 상당 시간 가격이 회복하지 않자 알고리즘에 대해 신뢰를 거둔 사용자들이 UST를 LUNA로 교환하여 거래소에 덤핑하면서 LUNA의 가치는 폭락하였고 UST는 다시 1$에 페깅되지 못하고 동반하락하고 말았다. 이는 알고리즘 스테이블 코인이 디페깅을 빠른 시간 안에 회복하지 못하면 시장의 신뢰를 잃어 가격을 유지하는 알고리즘이 감당할 수 없는 수준까지 물량이 나올 수 있다는 것을 증명한다. 트론 네트워크에서 운영되는 USDD 또한 UST와 동일한 위험요인을 가지고 있지만 LUNA 사태 이후에도 가격유지에 성공하고 있다. 하지만 22년 11월 현재 미세한 디페깅 상태(0.98~0.99달러)를 유지하고 있어서 향후 디페깅이 더 커질 위험이 높은 상황이다. 이를 방어하기 위해 USDD의 발행사는 준비금을 130%로 유지하겠다고 발표했고 준비금에 있는 USDC를 매도하여 USDD 가격 유지에 필요한 TRX를 매수하고 있지만 아직까지 디페깅 상태가 완전히 회복되지 않고 있다.

FRAX의 경우 22년 11월 현재 담보비율이 93%로 매우 높은 편이다. 이는 현재 FRAX의 수요가 적다는 것을 의미한다. 이때는 담보가 방어 역할을 할 수 있기 때문에 신뢰성 이슈가 발생해도 디페깅이 일어날 확률이 매우 작다. 하지만 UST처럼 시장의 수요가 많을 때 갑자기 신뢰성이 사라진다면 FRAX의 담보비율이 낮은 상태에서 사용자들이 FRAX를 담보로 바꾸어가는 뱅크런 상황이 되므로 결국 FRAX의 페깅은 깨지게 될 것이다. 이런 경우라도 일부 USDC의 비중이 있으므로 FXS의 가격하락 속도가 LUNA에 비해서 느릴 것이기 때문에 이때 알고리즘이 개입하여 가격이 회복될 확률이 좀 더 높다고 판단할 수 있다.

### 2.3 Depegging due to failure of algorithm

FEI의 경우 출시 후 활성화를 위해 코인을 발행한 초기 사용자에게 할인 발행을 했는데, 해당 물량에는 판매제한을 걸어두어 추후 정상 가격으로 FEI가 발행할 때까지 다시 ETH로 바꾸지 못하도록 알고리즘을 구성하여 투기성 환매를 방지하였다. 하지만 FEI가 출시 직후 중앙화된 거래소에 상장되면서 거기서 매도했을 때는 패널티를 회피할 수 있었고 초기 구매자들이 대량으로 매도하면서 가격이 하락하였다. 유니스왑풀의 또한 거래소의 가격을 오라클로 받아와서 거래하기 때문에 FEL의 가격은 출시 이후 1$를 회복하지 못하고 0.72$까지 하락하였다. 이는 신뢰성보다 알고리즘을 애초에 잘못 설계했기 때문에 발생한 문제이다. 현재는 알고리즘을 수정하여 페깅을 회복한 상태이다.

### 2.4 Liquidation due to high volatilty

청산 문제는 암호화폐 담보 스테이블코인들이 대부분 가지고 있는 위험요소이다. 이 문제를 회피하기 위해서 DAI, LUSD와 같이 비교적 가격변동성이 낮은 ETH를 담보로 스테이블코인을 발행하는 경우가 대부분이다. 그러므로 ETH보다 가격변동성이 큰 SNX를 담보로 하는 sUSD의 경우 좀 더 청산가능성이 높다고 판단할 수 있다. 21년 5월 19일 BTC를 비롯하여 대다수의 코인가격이 순간적으로 40% 이상 하락하는 사태가 발생했는데, 이후 BTC를 비롯하여 암호화폐 가격은 회복했지만 당시 순간적인 폭락으로 많은 담보들이 청산되면서 많은 피해자들이 발생했다. 드물지만 각국 정부의 규제이슈나 각종 악재가 발생할 경우 가격 변동이 매우 심한 경우가 발생하는 경우가 있기 때문에 암호화폐 담보 스테이블코인의 사용자들은 자본 비효율성을 감수하더라도 위험수준을 염두에 두고 여유 있게 담보비율을 유지해야 한다.

### 2.5 Oracle Attack

암호화폐 담보 스테이블코인은 오라클의 가격정보를 이용하여 담보의 청산을 결정하기 때문에 오라클 공격의 위험에 노출되어 있다. 일부 알고리즘 스테이블코인 또한 오라클의 가격정보를 참고하므로 동일한 위험에 노출되어 있다. 공격자들은 오라클의 데이터 소스가 되는 거래소에서 매수/매도를 통해 가격을 조작하여 담보의 가치를 낮춰서 낮은 가격에 담보를 가지고 오거나 청산 물량으로 나오는 담보를 싸게 매집하는 등의 방법으로 이윤을 창출한다. 이는 근본적으로 암호화폐 담보 스테이블코인의 운영체계를 무너뜨리는 것이기 신뢰성 문제를 발생시키며 디페깅으로 연결될 수 있다.

최근에 LINK와 같은 오라클 솔루션들이 가격 조작방지 기술들을 도입하면서 오라클 공격에 대한 가능성이 많이 감소했다. 하지만 상장된 거래소가 적어 오라클이 참조할 수 있는 데이터소스가 부족하고 시총이 작은 코인들은 가격의 조작의 가능성이 여전히 존재한다. 그러므로 이런 코인들을 담보로 발행되는 스테이블코인은 오라클공격의 위험성에 노출되어 있다. 22년 11월 솔라나 블록체인 기반의 스테이블코인 USDH가 오라클 공격을 받아 126만 달러의 손실이 발생한 것이 최근 대표적인 피해사례이다.

## V. Conclusion

스테이블코인은 현실세계의 통화와 블록체인 내의 암호화폐의 연결고리를 하는 중요한 요소이다. 법정화폐를 담

보로 발행된 코인에서 시작된 스테이블코인은 중앙화 이슈를 보완하기 위해 스마트 계약으로 발행되는 암호화폐 기반의 스테이블코인으로 발전했다. 하지만 담보비율로 인한 비효율성 문제는 여전히 존재했다. 이를 보완할 수 있는 알고리즘 스테이블코인이 출시되었지만 BAC, UST처럼 디페깅이 발생하여 대부분 사장되고 말았다. 결국 순수 알고리즘 스테이블코인은 결국 성공사례가 없다고 볼 수 있고 하이브리드 스테이블코인인 FRAX, FEI는 결국 담보가 가격을 유지시켜준다는 점에서 한계가 있지만 담보의 효율성을 개선했다는 측면에서 반쪽의 성공이라고 판단할 수 있다. 본 연구를 통해 분석된 위험요인들이 보완되어 지금보다 더 견고하고 효율적인 스테이블코인 프로젝트들이 나타나길 기대한다.

## REFERENCES


[1] A. Briola, D. Vidal-Tomás, Y. Wang, and T. Aste, “Anatomy of a Stablecoin’s failure: The Terra-Luna case,” Finance Research Letters, vol. 51. Elsevier BV, p. 103358, Jan. 2023. doi: 10.1016/j.frl.2022.103358.

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf

[3] J. Kim, “A Survey of Cryptocurrencies based on Blockchain,” Journal of the Korea Society of Computer and Information, vol. 24, no. 2, pp. 67-74, Feb. 2019. doi:10.9708/JKSCI.2019.24.02.067.

[4] Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform-Ethereum Whitepaper“, 2014. https://github.com/ethereum/wiki/wiki/White-Paper

[5] J. Kim and S. Kim, “A Survey of Decentralized Finance(DeFi) based on Blockchain,” Journal of the Korea Society of Computer and Information, vol. 26, no. 3, pp. 59-67, Mar. 2021. doi: 10.9708/JKSCI.2021.26.03.059.

[6] V. Mohan, “Automated market makers and decentralized exchanges: a DeFi primer,” Financial Innovation, vol. 8, no. 1. Springer Science and Business Media LLC, Feb. 2022. doi: 10.1186/s40854-021-00314-5.

[7] Breidenbach, Lorenz, et al., Chainlink 2.0: Next steps in the evolution of decentralized oracle networks., https://research.chain.link/whitepaper-v2.pdf

[8] Band Protocol Whitepaper, https://docs.bandchain.org/whitepaper/

[9] K. Ito, M. Mita, S. Ohsawa, and H. Tanaka, “What is Stablecoin?: A Survey on Its Mechanism and Potential as Decentralized Payment Systems,” International Journal of Service and Knowledge Management, vol. 4, no. 2. International Institute of Applied Informatics, pp. 71-86, 2020. doi: 10.52731/ijskm.v4.i2.574.

[10] Kahya, Ayten, Bhaskar Krishnamachari, and Seokgu Yun. *"Stablecoins: Reducing the Volatility of Cryptocurrencies."* Handbook on Blockchain. Springer, Cham, pp. 445-461, 2022. doi: 10.1007/978-3-031-07535-3_14

[11] Zhu, Jin, et al. "A Survey of Blockchain-Based Stablecoin: Cryptocurrencies and Central Bank Digital Currencies." International Conference on Blockchain and Trustworthy Systems. Springer, pp. 177-193, Dec, 2022. doi: 10.1007/978-981-19-8043-5_13

[12] Bordo, Michael D., and William Roberds. *“Central Bank Digital Currencies, an Old Tale With a New Chapter.”* No. w30709. National Bureau of Economic Research, 2022. doi: 10.3386/w30709


## Author

Junsang Kim received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Hanyang University, Korea, in 2003, 2005 and 2017, respectively. Dr. Kim is currently an assistant professor of Department of Cyber Science at Korea Naval Academy. He is interested in Blockchain, Big Data, and Cloud Computing technology.